РАДИОТЕХНИКА

УДК 621.391

МЕТОДЫ ФОРМИРОВАНИЯ БЛОЧНЫХ ЦИКЛИЧЕСКИХ КОДОВ

О.А. Гомцян

Национальный политехнический университет Армении

Рассмотрены вопросы построения систематических и несистематических циклических кодов, применяемых во многих современных системах обработки информации, таких как передача аудио- и видеоинформации; запись и считывание на CD, DVD; компьютерные сети и др. Блочные циклические коды – это избыточные коды, при построении которых к информационным символам добавляются корректирующие символы, что дает возможность обнаруживать и исправлять ошибки. Корректирующая способность таких кодов зависит от системы правил, применяемых для их построения, а также от длины кода, числа избыточных символов и др. В циклических кодах каждая новая комбинация формируется путем сдвига предыдущей, разрешенной вправо или влево на один разряд. При этом полученная комбинация является также разрешенной. При исследовании циклических кодов удобным алгебраическим средством их описания являются полиномы, так как имеется возможность применения известных преобразований над полиномами. Основой формирования этих кодов служат генераторные многочлены, которые выбираются из соответствующих неприводимых полиномов. Неприводимым является полином, который не разложим на многочлены более низшей степени. Это означает, что такой полином делится только на единицу и на самого себя. Техническая реализация таких кодов достаточно простая, так как основана на регистрах свига. Однако, несмотря на простоту реализации, математический аппарат для описания этих кодов довольно сложный. Известно, что процедура декодирования является более сложной, чем процесс кодирования. Достаточно простым для циклических кодов является декодирование, которое основано на вычислении синдрома. В работе, используя правила операций над полиномами, на разных примерах показаны методика и особенности построения циклических кодов.

Ключевые слова: корректирующий код, циклический код, кодовое слово, генераторный многочлен, систематический и несистематический коды.

Введение. В настоящее время существует большое количество избыточных кодов, применяемых для контроля (т.е. обнаружения и исправления) ошибок, среди которых выделим блочные [1-3].

Основная идея блочных кодов проиллюстрирована на рисунке.

Здесь из незакодированной входной импульсной последовательности "вырезаются" блоки, каждый длительностью k информационных символов. Далее в кодере к ним добавляются так называемые контролирующие

(проверочные, корректирующие, избыточные, исправляющие) символы r так, что общая длина кода равна $n = k + r$. Многочисленное количество различных контролирующих кодов отличается друг от друга, в основном, способами получения избыточных символов, которые позволяют корректировать ошибки.

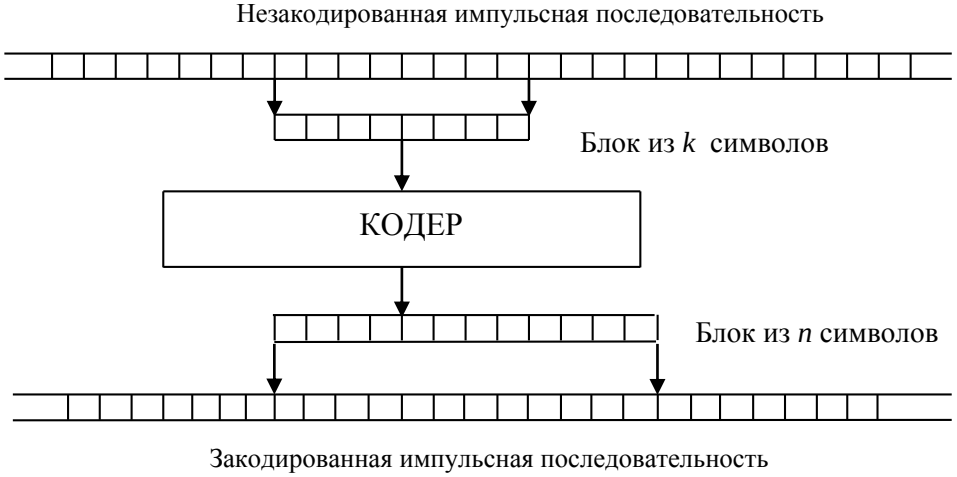

Рис. Процесс избыточного кодирования

В работе рассматриваются основные способы формирования проверочных символов для систематических и несистематических циклических кодов (ЦК).

Математический аппарат. Наиболее распространенными кодами с обнаружением и исправлением ошибок являются циклические коды, обладающие рядом достоинств, которые выделяют их среди остальных кодов. Они имеют более компактное описание, чем другие линейные коды, позволяют обнаруживать и исправлять кратные ошибки и очень эффективны для контроля серийных (пакетов) ошибок. Схемы кодеров и декодеров достаточно просты и могут быть реализованы с помощью обычных регистров сдвига.

Главная идея этих кодов заключается в том, что циклический сдвиг любого кодового слова (КС) приводит к новому КС. Например, если $(c_1, c_2, ..., c_{n-1}, c_n)$ - это КС, то кодовыми словами также являются $(c_2, c_3, ..., c_n, c_1)$; $(c_3, c_4, ..., c_1, c_2)$ и т.д., которые сформированы циклическим сдвигом разрядов влево (можно сдвигать и вправо). В общем случае циклический сдвиг разрядов, например, влево на r позиций может быть записан как $(c_{r+1}, c_{r+2}, ..., c_n, c_1, c_2, ..., c_r)$.

Аналитическое описание и преобразования над циклическими кодами удобно осуществлять, представив их в следующей полиномиальной форме [2,4]:

$$c(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{n-1} x^{n-1}, \quad (1)$$

где x - основание КС (фиктивная переменная); c_i - координаты КС (для двоичных кодов – это 0 и 1), причем n - его длина.

Циклический сдвиг этого полинома вправо можно получить, умножив его на x. Действительно,

$$xc(x) = c_0 x + c_1 x^2 + c_2 x^3 + ... + c_{n-2} x^{n-1} + c_{n-1} x^n = c^{(1)}(x). \quad (2)$$

Чтобы степень полинома не превышала $n-1$, необходимо в этом выражении положить $x^n = 1$. Тогда получим циклический сдвиг, например, на один разряд вправо:

$$c^{(1)}(x) = xc(x) = c_{n-1} + c_0 x + c_1 x^2 + c_2 x^3 + ... + c_{n-2} x^{n-1}. \quad (3)$$

Сдвиг на два разряда дает

$$c^{(2)}(x) = x^2 \cdot c(x) = c_{n-2} + c_{n-1} x + c_0 x^2 + c_1 x^3 + ... + c_{n-3} x^{n-1} . \quad (4)$$

В общем случае при сдвиге на $n-1$ разряд получим

$$c^{(n-1)}(x) = c_1 + c_2 x + c_3 x^2 + ... + c_0 x^{n-1} . \quad (5)$$

Кодирование и декодирование циклических кодов можно производить с помощью матриц, а также методом, основанным на понятии генераторного (порождающего, образующего, производящего) полинома.

Представление циклических кодов с помощью генераторного полинома. Сущность этого метода заключается в том, что кодовый полином $c(x)$ (а следовательно, и КС) формируется умножением информационного кодового слова длиной k, выраженного в виде полинома $m(x)$ степени $k-1$, на генераторный полином $g(x)$ степени $r = n - k$. Естественно, что при делении КС (т.е. разрешенной комбинации) на генераторный полином мы получим нулевой остаток. Если же кодовое слово исказилось под влиянием ошибок, т.е. образовалась запрещенная комбинация, то результат аналогичного деления даст некоторый остаток, по которому и можно судить о наличии ошибок. Отметим, что в систематических ЦК, в отличие от несистематических, позиции проверочных и информационных символов строго определены. Вначале в КС могут располагаться проверочные, а затем информационные символы, или наоборот.

Итак, напомним некоторые положения из теории ЦК. Опишем информационный, генераторный и кодовый полиномы в виде

$$m(x) = m_0 + m_1 x + m_2 x^2 + ... + m_{k-1} x^{k-1} , \quad (6)$$

$$g(x) = g_0 + g_1 x + g_2 x^2 + ... + g_r x^r , \quad (7)$$

$$c(x) = c_0 + c_1 x + c_2 x^2 + ... + c_{n-1} x^{n-1} . \quad (8)$$

Перепишем полином $m(x)$ следующим образом:

$$m(x) = c_{n-k}x^{n-k} + c_{n-k+1}x^{n-k+1} + ... + c_{n-1}x^{n-1}, \quad (9)$$

т.е. информационные символы здесь расположены в конце КС. Тогда проверочный полином будет иметь вид

$$p(x) = c_0 + c_1x + c_2x^2 + ... + c_{n-k-1}x^{n-k-1}, \quad (10)$$

т.е. проверочные символы здесь занимают первые позиции КС. В результате получим систематический ЦК в общем виде:

$$\begin{aligned} c(x) = p(x) + m(x) = c_0 + c_1x + ... + c_{n-k-1}x^{n-k-1} + \\ + c_{n-k}x^{n-k} + c_{n-k+1}x^{n-k+1} + ... + c_{n-1}x^{n-1} = \sum_{i=0}^{n-1} c_i x^i. \end{aligned} \quad (11)$$

Для формирования *несистематических* ЦК обычно используется следующее простое выражение:

$$c(x) = m(x) \cdot g(x). \quad (12)$$

Рассмотрим способ построения *систематических* циклических кодов. Как уже отмечалось ранее, последовательные сдвиги $x^r \cdot c(x)$ кодового слова $c(x)$ образуют также новое кодовое слово. Умножив $m(x)$ на $g(x)$ и разделив результат на x^r, получим

$$\frac{x^r \cdot m(x)}{g(x)} = \varepsilon(x) + \frac{\rho(x)}{g(x)}, \quad (13)$$

где $\varepsilon(x)$ - частное от деления; $\rho(x)$ - остаток.

При делении степень частного $\varepsilon(x)$ равна степени $m(x)$, т.е. $k-1$, т.к. степени x^r и $g(x)$ одинаковы. Степень же остатка не может превысить степень $g(x)$ и равна $(r-1)$. Из выражения (13) нетрудно получить

$$\varepsilon(x) \cdot g(x) = x^r \cdot m(x) - \rho(x) = c(x). \quad (14)$$

Так как сложение и вычитание по модулю равнозначны, то в дальнейшем будем использовать в этой формуле знак “плюс”.

Как отмечалось выше, степень полинома $\rho(x)$ равна степени полинома $m(x)$. Поэтому произведение $\varepsilon(x) \cdot g(x)$ также дает кодовое слово, что и произведение $m(x) \cdot g(x)$. Следовательно, выражение (14) может быть записано в виде

$$c(x) = m(x) \cdot g(x) = x^r \cdot m(x) + \rho(x), \quad (15)$$

где $\rho(x)$ - остаточный полином, который является проверочным со степенью, меньшей или равной $r-1$. Далее, объединив (11) и (15), получим выражение для систематического кода:

$$c(x) = \rho(x) + x^{n-k} m(x) = \\ = \rho_0 + \rho_1 x + \ldots + \rho_{n-k-1} x^{n-k-1} + m_0 x^{n-k} + m_1 x^{n-k+1} + \ldots + m_{k-1} x^{n-1}, \quad (16)$$

которому соответствует кодовое слово

$$C = (\rho_0, \rho_1, \ldots, \rho_{n-k-1}, m_0, m_1, \ldots, m_{k-1}),$$

или в общем виде $C = (c_0, c_1, c_2, \ldots, c_{n-2}, c_{n-1})$.

Результаты исследования. Используем приведенные соотношения с целью построения циклического кода ЦК(7,4) для следующих информационных кодовых слов: $m_1(x) = 1 + x + x^2$; $m_2(x) = x + x^3$; $m_3(x) = 1 + x + x^2 + x^3$ и $m_4(x) = x^3$. Здесь имеем $n = 7$, $k = 4$ и $r = 7 - 4 = 3$. Определим генераторный полином, разложив двучлен $x^n \pm 1 = x^{2^m - 1} \pm 1$ на неприводимые полиномы [1]. Для нашего случая найдем, что $m = 3$. Это значит, что сомножителями двучлена $x^7 + 1$ должны быть неприводимые полиномы, степени которых являются делителями числа 3, т.е. это полиномы первой и третьей степеней. Тогда, используя таблицы неприводимых полиномов, получим следующее разложение [1]:

$$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

Для кода ЦК(7,4) генераторный полином должен иметь степень $r = 3$. Остановим выбор на полиноме $g(x) = 1 + x^2 + x^3$, т.е. кодовый вектор (КВ) равен $G = 1011$. Теперь определим кодовые комбинации для всех заданных информационных кодовых слов, используя формулу (12).

Для $m_1(x) = 1 + x + x^2$ (КВ $M_1 = 1110$) имеем

$c_1(x) = (1 + x + x^2)(x^3 + x^2 + 1) = 1 + x + x^5$, т.е. $C_1 = 1100010$.

Далее $m_2(x) = x + x^3$ (КВ $M_2 = 0101$). Аналогично:

$$c_2(x) = (x + x^3)(x^3 + x^2 + 1) = x + x^4 + x^5 + x^6, \text{ т.е. } C_2 = 0100111.$$

Следующий код для $m_3(x) = 1 + x + x^2 + x^3$ (КВ $M_3 = 1111$) имеет вид

$c_3(x) = (1 + x + x^2 + x^3)(x^3 + x^2 + 1) = 1 + x + x^3 + x^6$, т.е. $C_3 = 1101001$.

И, наконец, для $m_4(x) = x^3$ (КВ $M_4 = 0001$) имеем

$$c_4(x) = x^3(x^3 + x^2 + 1) = x^3 + x^5 + x^6, \text{ т.е. } C_4 = 0001011.$$

Обратив внимание на структуру полученных кодовых слов, заметим, что здесь ни первые k позиций, ни последние не занимают информационные кодовые слова, а это значит, что полученный код *несистематический*.

Заметим, что если мы будем записывать все полиномы в виде $f(x)=f_1x^{n-1}+f_2x^{n-2}+...+f_n$, т.е. по убывающим степеням переменной x, то в результате получим кодовые слова, инверсные тем, что получены нами. Например, для $m_2^{'}(x)=x^3+x,$ т.е. $M_2^{'}=1010,$ имеем кодовое слово $c_2^{'}(x)=x^6+x^5+x^4+x$ и вектор $C_2^{'}=1110010,$ инверсный с кодовым словом C_2 .

Теперь построим одно кодовое слово для *систематического* кода ЦК(7,4), используя предыдущий генераторный полином. Пусть $m_1(x)=1+x+x^2$ или $M_1=1110.$ Тогда $x^3\cdot m_1(x)=x^3\cdot(1+x+x^2)=x^3+x^4+x^5$.

Разделив этот результат на $g(x)$ в соответствии с формулой (13):

$$\begin{array}{l} x^3+x^4+x^5 \;\big|\; \underline{1+x^2+x^3} \\ \underline{x^2+x^4+x^5} \quad x^2+1 \longrightarrow \varepsilon_1(x) \\ \quad x^2+x^3 \\ \underline{1+x^2+x^3} \\ \quad 1 \longrightarrow \rho_1(x), \end{array}$$

получим кодовое слово по формуле (15):

$$c_1(x)=\rho_1(x)+x^r\cdot m_1(x)=1+x^3+x^4+x^5,\ \text{т.е.}\ C_1=1001110.$$

Как уже отмечалось, существует различное представление полиномов, а именно, по возрастающим или по убывающим степеням переменной *x.* Рассмотрим теперь предыдущий пример для случая убывания степеней x. Для этого построим одно КС для систематического кода ЦК(7,4), используя для генераторного и информационного полиномов соответственно записи $g(x)=x^3+x^2+1$ и $m_1(x)=x^2+x+1$ (т.е. $M_1=0111$).

Тогда $x^3\cdot m_1(x)=x^3\cdot(x^2+x+1)=x^5+x^4+x^3$. Произведем деление

$$\begin{array}{l} x^5+x^4+x^3 \;\big|\; \underline{x^3+x^2+1} \\ \underline{x^5+x^4+x^2} \quad x^2+1 \longrightarrow \varepsilon_1(x) \\ \quad x^3+x^2 \\ \quad x^3+x^2+1 \\ \quad \underline{\qquad\qquad} \\ \qquad 1 \longrightarrow \rho_1(x). \end{array}$$

Окончательно имеем $c_1(x) = x^5 + x^4 + x^3 + 1 = 0111001$, т.е. первые $k = 4$ позиции занимает информационный вектор, а следующие $r = 3$ – проверочный вектор (остаток), причем, что очень важно, кодовые слова инверсны друг другу!

Покажем еще, что $c_1(x)$ можно получить также и простым перемножением $\varepsilon_1(x)$ на $g(x)$. Действительно,

$$\varepsilon_1(x) \cdot g(x) = (1 + x^2)(1 + x^2 + x^3) = 1 + x^2 + x^3 + x^2 + x^4 + x^5 = 1 + x^3 + x^4 + x^5.$$

В заключение, используя описанную методику, построим полный систематический циклический код ЦК(7,4) с генераторным полиномом $g(x) = 1 + x + x^3$. Результаты расчетов сведены в таблицу.

Так как количество проверочных символов $r = 3$, то возможно иметь всего 8 проверочных кодовых комбинаций, каждая из которых используется дважды при формировании кода ЦК(7,4).

Из этой таблицы также видно, что кодовое расстояние между любой парой кодовых слов равно $d_{min} = 3$. Кроме того, векторы 1111111 и 0000000 при циклическом сдвиге не изменяются. Остальные кодовые слова формируются циклическим сдвигом влево или вправо любых кодовых слов. Например, начиная с кодового слова C_8, которое соответствует $M_8 = 1000$, последовательным сдвигом влево получим следующую цепочку кодовых векторов (стрелки указывают направление сдвига):

1101000 (N8) ←1010001 (N1)← 0100011(N3) ←1000110(N6) ← 0001101(N13) ←
←0011010(N10) ← 0110100(N4) ←1101000(N8).

Сдвиг вправо дает реверсивную цепочку:

1101000(N8)→0110100(N4)→0011010(N10)→0001101(N13)→1000110(N6) →
→0100011(N3) →1010001(N1) →1101000(N8).

Или другой пример: начав с кодового слова C_{14}, которое соответствует $M_{14} = 1110$, получим

0101110←1011100←0111001←1110010←1100101←1001011←0010111←0101110.

Анализ этих результатов показывает, что кодовые векторы в цепочке располагаются случайным образом и зависят от порядка следования информационных КС.

Таким образом, построили полный систематический код ЦК(7,4).

Таблица.

Систематический код ЦК(7,4)

Номера КС	Векторы информационных КС $M = m_0m_1m_2m_3$	Полиномы информационных КС $m(x) = 1 + x + x^2 + x^3$	Векторы кода $C = c_0c_1c_2c_3c_4c_5c_6$	Полиномы кода $c(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$
0	0 0 0 0	0	0 0 0 0 0 0 0	0
1	0 0 0 1	x^3	1 0 1 0 0 0 1	$1 + x^2 + x^6$
2	0 0 1 0	x^2	1 1 1 0 0 1 0	$1 + x + x^2 + x^5$
3	0 0 1 1	$x^2 + x^3$	0 1 0 0 0 1 1	$x + x^5 + x^6$
4	0 1 0 0	x	0 1 1 0 1 0 0	$x + x^2 + x^3$
5	0 1 0 1	$x + x^3$	1 1 0 0 1 01	$1 + x + x^4 + x^6$
6	0 1 1 0	$x + x^2$	1 0 0 0 1 1 0	$1 + x^4 + x^5$
7	0 1 1 1	$x + x^2 + x^3$	0 0 1 0 1 1 1	$x^2 + x^4 + x^5 + x^6$
8	1 0 0 0	1	1 1 0 1 0 0 0	$1 + x + x^3$
9	1 0 0 1	$1 + x^3$	0 1 1 1 0 0 1	$x + x^2 + x^3 + x^6$
10	1 0 1 0	$1 + x^2$	0 0 1 1 0 1 0	$x^2 + x^3 + x^5$
11	1 0 1 1	$1 + x^2 + x^3$	1 0 0 1 0 1 1	$1 + x^3 + x^5 + x^6$
12	1 1 0 0	$1 + x$	1 0 1 1 1 0 0	$1 + x^2 + x^3 + x^4$
13	1 1 0 1	$1 + x + x^3$	0 0 0 1 1 0 1	$x^3 + x^4 + x^6$
14	1 1 1 0	$1 + x + x^2$	0 1 0 1 1 1 0	$x + x^3 + x^4 + x^5$
15	1 1 1 1	$1 + x + x^2 + x^3$	1 1 1 1 1 1 1	$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$

Заключение. Приведена методика конструирования систематических и несистематических циклических кодов, основанная на использовании генераторного полинома. Показано, что если полиномы представлены по убывающим степеням переменной x, то первые k позиций кодового слова

(считая слева направо) занимают информационные символы, остальные r позиций – проверочные символы. В случае же описания полиномов по возрастающим степеням x на первых r позициях располагаются проверочные символы, а на последних k позициях – информационные символы. Окончательный выбор - за исследователем.

Литература

1. **Питерсон У., Уэлдон Э.** Коды, исправляющие ошибки / Пер. с англ.; Под ред. Р.Л. Добрушина и С.И. Самойленко. – М.: Мир, 1976.- 594 с.
2. **Wicker S.B.** Error Control Systems for Digital Communication and Storage.- Englewood Cliffs, N. J.: Prentice-Hall, 1994.- 503 p.
3. **Скляр Б.** Цифровая связь. Теоретические основы и практическое применение. 2-е изд. / Пер. с англ.- М.: Издательский дом “Вильямс”, 2003.- 1104 с.
4. **Гомцян О.А.** Способы построения циклических кодов // Сборник материалов годичной научной конференции ГИУА. - Ереван, 2002. – Т.2. - С. 399-401.

Поступила в редакцию 25.02.2016.
Принята к опубликованию 20.05.2016.

ԲԼՈԿԱՅԻՆ ՑԻԿԼԻԿ ԿՈԴԵՐԻ ՁԵՎԱՎՈՐՄԱՆ ԵՂԱՆԱԿՆԵՐԸ

Հ.Ա. Գոմցյան

Դիտարկվել են պարբերական և ոչ պարբերական ցիկլիկ կոդերի կառուցման հարցերը, որոնք կիրառվում են ինֆորմացիայի մշակման ժամանակակից բազմաթիվ համակարգերում, ինչպիսիք են աուդիո և վիդեո ինֆորմացիայի հաղորդումը, գրանցումը և վերարտադրումը CD և DVD-ներում, համակարգչային ցանցերը և այլն: Բլոկային ցիկլիկ կոդերը հավելուրդով կոդեր են, որոնց կառուցման ժամանակ ինֆորմացիոն սիմվոլներին գումարվում են շտկող սիմվոլները, ինչը թույլ է տալիս հայտնաբերել և շտկել սխալները: Այդպիսի կոդերի շտկող հատկությունը կախված է այն կանոնների համակարգից, որոնք օգտագործվում են դրանց կառուցման համար, ինչպես նաև կոդի երկարությունից, հավելյալ նիշերի թվից և այլն: Ցիկլիկ կոդերում ամեն մի նոր կոնբինացիա ձևավորվում է նախորդ թույլատրված կոմբինացիայի՝ մեկ կարգով աջ կամ ձախ շեղմամբ: Ընդ որում, ստացված կոնբինացիան նույնպես համարվում է թույլատրված: Ցիկլիկ կոդերը հետազոտելիս դրանց նկարագրման հանրահաշվական հարմար միջոց են բազմանդամները, քանի որ հնարավոր է օգտագործել բազմանդամների հայտնի ձևափոխությունները: Այդ կոդերի հիմք են ծառայում գեներատորային բազմանդամները, որոնք ընտրվում են համապատասխան չբերվող պոլինոմներից: Չբերվող է այն բազմանդամը, որը չի բաղադրվում ավելի ցածր աստիճանի բազմանդամների: Դա նշանակում է, որ այդպիսի բազմանդամները բաժանվում են միայն մեկի և իրենց վրա: Այդպիսի կոդերի տեխնիկական իրականացումը բավական պարզ է, քանի որ հիմնված է տեղաշարժվող ռեգիստրների վրա: Չնայած իրականացման պարզությանը, այդ կոդերի նկարագրման համար մաթեմատիկական ապարատը բավա-կան բարդ է:

Հայտնի է, որ ապակոդավորման գործողությունը ավելի բարդ է, քան կոդավորման գործընթացը: Բավական պարզ է ցիկլիկ կոդերի ապակոդավորումը, որը հիմնված է սինդրոմի հաշվարկման վրա: Օգտագործելով բազմանդամների նկատմամբ գործողությունների կանոնները, տարբեր օրինակներով ցուցադրված են ցիկլիկ կոդերի կառուցման մեթոդաբանությունը և առանձնահատկությունները:

Առանցքային բառեր. շտկող կոդ, ցիկլիկ կոդ, կոդային բառ, գեներատորային բազմանդամ, պարբերական և ոչ պարբերական կոդեր:

METHODS FOR FORMING BLOCK CYCLIC CODES

H.A. Gomtsyan

Issues on constructing systematic and non-systematic cyclic codes used in many modern data processing systems, such as the transmission of audio and video information, reading and writing on CD, DVD, computer networks, etc are considered. Block cyclic codes are redundant codes, at whose construction, correcting symbols are added to the information symbols, allowing to detect and correct the errors. The correction ability of such codes depends on the system of the rules used for their construction, as well as the code length, the number of redundant symbols, etc. In cyclic codes, every new combination is generated by shifting the previous permissible one right or left by one digit. In this case, the resulting combination is also permissible. At studying the cyclic codes, polynomials are convenient means of algebraic descriptions, as it is possible to apply the known transformations of polynomials. The basis for the formation of these codes are the generator polynomials, which are selected from the corresponding irreducible polynomials. An irreducible polynomial is the one that does not expand on polynomials over a lower degree. This means that a polynomial is divisible only by one and by itself. The technical realization of such codes is quite simple, because it is based on shift registers. However, despite the ease of implementation, the mathematical instrument to describe these codes is rather complicated. It is known that the decoding procedure is more complicated than the encoding process. Simple enough for cyclic codes is decoding, which is based on the calculation of the syndrome. Using the rules of operations on polynomials, the methodology and features of constructing cyclic codes on different examples are shown.

Keywords: error correction code, cyclic code, code word, generator polynomial, systematic and non-systematic codes.